



UNITED STATES MARINE CORPS  
MARINE CORPS COMBAT DEVELOPMENT COMMAND  
QUANTICO, VIRGINIA 22134-5001

Canc: Oct 09

CDCBul 5239

B 01

24 Nov 2008

COMBAT DEVELOPMENT COMMAND BULLETIN 5239

From: Commanding General  
To: Distribution List

Subj: HANDLING, SAFEGUARDING, AND REPORTING BREACHES OF  
PERSONALLY IDENTIFIABLE INFORMATION (PII)

Ref: (a) MCBul 5239 (MARADMIN 491/08)  
(b) The Privacy Act of 1974 (5 U.S.C. 552a) (as amended)  
(c) SECNAVINST M-5210.1

Encl: (1) Report of Theft/Loss/Compromise of Personally  
Identifiable Information (Template)  
(2) USMC PII Compliance Report  
(3) USMC PII Compliance Checklist

1. Purpose. To establish policy so as to balance the need of the Marine Corps Combat Development Command (MCCDC) to maintain information relevant to carrying out its myriad missions with the obligation to protect individuals against unwarranted invasions of their privacy stemming from the collection, maintenance, use, and disclosure of PII.

2. Information. PII refers to any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., and any other personal information which is linked or linkable to an individual.

3. Action. In addition to those commands, agencies, and divisions specified below, all personnel assigned to MCCDC organizations will adhere to the policies and guidelines contained herein, as well as references (a) and (b). It is therefore incumbent upon all personnel, military and civilian, to ensure they are aware of the proper methods of handling and safeguarding PII as well as the procedures to take should a breach occur.

a. Assistant Chief of Staff, G-1. Develop and implement MCCDC-wide policy in accordance with reference (a) regarding the handling and safeguarding of PII.

24 Nov 08

b. MCCDC/Marine Corps Base (MCB) Quantico Privacy Act Coordinator

(1) Advise commanders and supported agencies, as necessary, to ensure appropriate action is taken in the event a breach involving PII occurs within the MCCDC AOR.

(2) In the event of a breach, advise Commanders and supported Agencies, as necessary, on the proper method for completing and submitting a Report of Theft/Loss/Compromise of PII (enclosure (1)), as well as all reporting requirements contained in reference (a), to appropriate agencies.

c. Director, Communications Division, G-6

(1) Execute clean-ups of PII spillages on non-Navy Marine Corps Intranet (NMCI) networks.

(2) Serve as the liaison between MCCDC, HQMC Command, Control, Communications, and Computers (C4), Marine Corps Network Operations and Security Command, and NMCI regarding execution of PII spillage clean-ups on NMCI and non-NMCI networks.

(3) Ensure the MCCDC Information Assurance Manager (IAM) tracks and reports completion of annual training and compliance reviews no later than 21 December of each year using the USMC PII Compliance Report (enclosure (2)).

d. Inspector General. Ensure the USMC PII Compliance Checklist is incorporated into the Privacy Act Functional Area portion of the Commanding General Validation Program.

e. Commanding Generals and Commanding Officers

(1) Appoint, in writing, an officer, staff non-commissioned officer, or civilian Marine (GS-7 and above) as the command/agency/directorate point of contact for PII and provide a copy of the appointment letter to the MCCDC/MCB Quantico Privacy Act Coordinator (Bldg 3250 (Lejeune Hall), Suite 109).

(2) Ensure the provisions of paragraphs 4a and 4b to reference (a) pertaining to the handling and safeguarding of PII are fully implemented. Specifically, you are directed to:

(a) Ensure all documents containing PII are marked "FOR OFFICIAL USE ONLY (FOUO)" on each page.

(b) Ensure any PII stored on network resources/ devices in shared folders are, at a minimum, password protected and only available to those individuals with an authorized business need to know.

(c) Ensure PII is not stored in public folders or any other folders/locations with unrestricted access.

(d) Ensure PII records are maintained in accordance with the appropriate Standard Subject Identification Code contained in reference (c).

(e) Ensure PII is not maintained on personally owned computers/devices.

(f) Ensure e-mail, to include attachments, containing any amount of PII is digitally signed and encrypted using Department of Defense (DOD) approved certificates. FOUO will be included at the beginning of the subject line and the body of the e-mail will contain a statement notifying the recipient to treat the e-mail and its contents as "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE." Any misuse or unauthorized access may result in both civil and criminal penalties.

(g) Ensure PII created, maintained, or manipulated on any mobile device (i.e., Blackberry, flash drive, external hard drive, cell phone, etc.) is encrypted through currently approved methods.

(h) Ensure PII is restricted to DOD owned, leased, or occupied workspaces. Should compelling operational needs require removal from the workplace, the laptop computer, mobile computing device, or removable storage media will:

1 Be signed in and out with a supervising official designated in writing by the Command.

2 Be configured to require certificate-based authentication for log-on (where possible).

3 Be set to implement screen lock, with a specified period of inactivity not to exceed 15 minutes (where possible).

(i) Ensure disposal methods for paper documents containing PII is adequate to ensure the information is left beyond reconstruction. Documents containing PII will not be disposed of in trash cans or recycling containers unless properly shredded.

24 Nov 08

(j) Ensure electronic storage devices containing PII are destroyed in such a manner as to render it unreadable and unusable. Such methods include degaussing, overwriting, or destroying the device.

(3) Ensure compliance with the provisions of paragraph 4c to reference (a) when a breach or compromise of PII occurs. Specifically, you are directed to:

(a) Within 1 hour of discovery of actual or suspected loss, theft, or compromise of PII, complete all information specified on the Report of Theft/Loss/Compromise of PII and report the information (via e-mail) to the agencies identified in paragraph 4c(1) through 4c(9) of reference (a). The MCCDC IAM (e-mail: [MCBQG6IA@usmc.mil](mailto:MCBQG6IA@usmc.mil)) and MCCDC/MCB Quantico Privacy Act Coordinator (e-mail: [MCBQuanticoFOIA@usmc.mil](mailto:MCBQuanticoFOIA@usmc.mil)) will be included as "Cc:" info addressees on the notification e-mail.

(b) Within 24 hours of the initial report, report the following information (via e-mail) to the agencies outlined in paragraph 3e(3)(a) above:

1 Report of the status of the Command's plan to notify individuals whose information was compromised.

2 Description of actions being taken to prevent future occurrences.

(c) Within 72 hours of the initial report, ensure a naval message is released to the DOD organizations identified in paragraph 4c(1) through 4c(9) of reference (a). The MCCDC IAM (PLAD: CG MCB QUANTICO VA G-6) and MCCDC/MCB Quantico Privacy Act Coordinator (PLAD: CG MCB QUANTICO VA G-1) will be included as "INFO:" addressees on the naval message.

(d) Within 10 days of the initial discovery of a known or suspected compromise, and on the direction of HQMC, notify the affected personnel of the loss. Paragraph 4c(9)(b) of reference (a) contains amplifying information.


(4) Ensure all personnel (Marines, civilians, and contractors) complete annual Defense Information Systems Agency (DISA) PII training (<http://www.quantico.usmc.mil/activities/?Section=IA>) and select

24 Nov 08

the PII training icon. Commands also have the option of directing their personnel to accomplish supplemental training located on the HQMC (C4) web-site (<https://hqodod.hqmc.usmc.mil/PII.asp?page=2008Standdown>).

(5) Conduct bi-annual reviews for compliance in the handling, storage, and destruction of PII within your AOR using the PII Compliance Checklist (enclosure (3)). These checklists will be kept on file by the Command for 3 years (current calendar year plus 2 calendar years) and will be an inspection item on future MCCDC/MCB Quantico Commanding General Validation Program visits.

(6) Provide the Director, Communications Division, G-6 IAM with a quantity of personnel who have completed the annual PII training, numbers of supplemental PII training completed, and number of compliance checks within their purview (see enclosure (2)) no later than 17 December of each year.

  
F. M. PADILLA  
Chief of Staff

DISTRIBUTION: A